DATA POWERS DIGITAL TRANFORMATION.
BE SURE IT'S PROTECTED.

Digital transformation is accelerating the pace of change. To keep up, retailers must place security at the forefront of their transformation strategy. However, 53% of retailers are deploying new technologies such as cloud, big data and IoT in advance of having next-generation security services in place.[1]

This is a risk no retailer should be willing to take.

Below are five security considerations driving the adoption of wavelength encryption technologies.

The Proliferation of IoT:

While retail deployments of IoT devices fuel big data analytics engines and business intelligence platforms, they generate tremendous amounts of sensitive company and customer data that must be collected, connected and securely distributed across the retail enterprise. According to Ovum, IT leaders cite data security and privacy concerns as the top barriers for successful IoT implementations.[2] Encrypted Layer 1 connectivity supports enhanced security of the transport infrastructure by safely routing critical data outside the data center to protect in-flight information across multiple protocols and all upper network layers.

Latency Is a Retail Killer:

Growing digital demands, increasing bandwidth consumption, big data and the proliferation of apps place pressure on IT teams to build and deploy secure and high-performing networking solutions. Existing 'in-flight' encryption options at the application layer (e.g. HTTPS/SSL) and Layer 3 (IPSec) seriously impact latency and limit scalability as retailers increase data consumption. In fact, 74% of enterprises cite system performance and latency as the most critical feature when considering encryption technology solutions.[3] And with 96% of retailers estimated to have end-to-end encryption by the end of 2019,[4] IT leaders must architect secure networking solutions that don't compromise performance — especially during peak season requirements. Today's on-demand, real-time retail environments require an efficient and low-latency network solution.

You're Only A Headline Away:

All it takes is one large-scale breach to erode customer confidence and damage brand reputation. According to IDC, over the next two years, 80% of consumers will defect from a business because their personally identifiable information (PII) is impacted in a security breach.[5] The digital data fueling digital transformation — PII, PAI, IP, credit card, loyalty programs, etc. — is attractive to cyber criminals looking to exploit security vulnerabilities. According to Gartner, "through 2020, driven by the increasing risk of a data breach, more than 50% of enterprises will purchase enterprisewide encryption products, which is a significant increase from fewer than 20% today."[6] Help protect company and customer data against "man in the middle attacks" through in-transit Layer 1 encryption across your interconnected data center and corporate locations.

Addressing Compliance Challenges:

While PCI DSS compliance is an important piece of the security checklist, it's not enough to protect retailers from rapidly evolving, sophisticated cyber threats. Today's retailers must deploy secure networking solutions that help deliver against regulatory requirements and protect customer information. In a recent report, 71% of U.S. retailers cited encryption as the top choice for satisfying data privacy regulations.[7] With vast amounts of omnichannel data traversing the network, wavelength encryption can help retailers ensure security compliance while creating an additional layer of defense. Building security into networking solutions will help retailers strengthen their security postures beyond PCI to stay ahead.

Reducing Complexity:

Omnichannel retailers are operating across more channels and transferring more data than ever before — creating complex security architectures and networks to manage and control. In fact, 44 percent of U.S. retailers cited complexity as the main barrier to securing sensitive data.[8] Today's IT leaders must design agile networks to ensure business continuity while also protecting critical information. Optical transport encryption services offered by network providers help retailers reduce overhead and management complexity by transitioning from on-premises hardware models to "encryption as a service." And with no need to buy or manage DWDM Encryption equipment or Key Management Service tools, retailers can free up IT resources and budgets to focus on business innovation.

LEVEL 3® ENCRYPTED WAVELENGTH SOLUTIONS: SECURE, EFFICIENT AND HIGH-PERFORMING

Contact Level 3 to learn more about implementing scalable, encrypted network connectivity to better protect your company and customer data.

[1] Thales Group, 2017 Thales Data Threat Report, Retail Edition, 2017
[2] Ovum, Integrating the IoT Economy, May 2017
[3] Ponemon Institute, Global Encryption Trends Study, April 2017
[4] BRP Consulting, POR/Customer Engagement Benchmarking Survey, 2017
[5] IDC Futurescape, Worldwide Security Products and Services Predictions, 2017
[6] Gartner, Prioritize Enterprise-Wide Encryption for Critical Datasets, 28 June 2017
[7] Thales Group, 2017 Thales Data Threat Report, Retail Edition, 2017
[8] Thales Group, 2017 Thales Data Threat Report, Retail Edition, 2017

Connecting and Protecting
the Networked World℠